PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2003-008589**
(43)Date of publication of application : **10.01.2003**

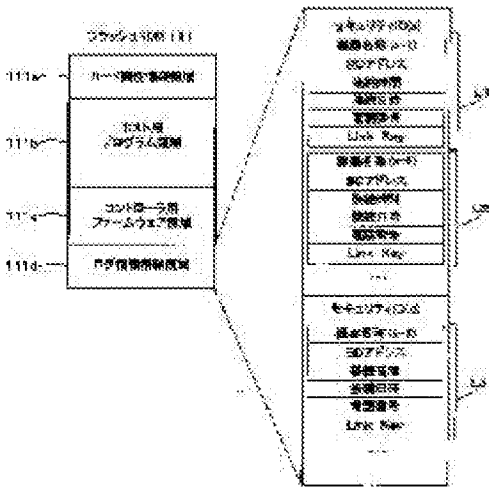
(51)Int.Cl. **H04L 12/28**
H04L 29/08
H04N 1/00
H04Q 7/38

(21)Application number : **2001-192179**
(22)Date of filing : **26.06.2001**

(71)Applicant : **TOSHIBA CORP**
(72)Inventor : **KOBAYASHI KOICHI**

(54) COMMUNICATION APPARATUS, COMMUNICATION SYSTEM AND COMMUNICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a communication apparatus having the same communication card that can simplify a radio communication link estabilishing job when connected to an external device having been connected before even if a host device mounted with the communication card differs.
SOLUTION: A log information storage area 111d is provided to a flash ROM 111 of an SD card 13 and stores log information when the SD card 13 is mounted to a host device such as a personal computer 1 and performs radio communication with an external device. Then when another host device such as a PDA 21 performs radio communication with the same external device, the host device downloads the log information from the log information storage area 111d so as to simplify radio link setup.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2003－8589
（P2003－8589A）
(43)公開日　平成15年１月10日(2003.1.10)

(51)Int.Cl.[7]		識別記号	Ｆ Ｉ		テーマコード（参考）
Ｈ０４Ｌ	12/28	３００	Ｈ０４Ｌ	12/28	３００Ｚ　５Ｃ０６２
	29/08		Ｈ０４Ｎ	1/00	１０７Ａ　５Ｋ０３３
Ｈ０４Ｎ	1/00	１０７	Ｈ０４Ｌ	13/00	３０７Ａ　５Ｋ０３４
Ｈ０４Ｑ	7/38		Ｈ０４Ｂ	7/26	１０９Ｒ　５Ｋ０６７

審査請求　未請求　請求項の数19　ＯＬ　（全 20 頁）

(21)出願番号　特願2001－192179(P2001－192179)

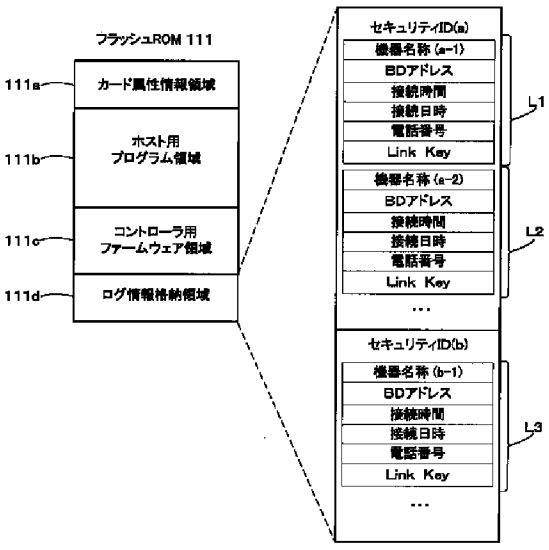
(22)出願日　平成13年６月26日(2001.6.26)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　小林　浩一
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内
(74)代理人　100083161
弁理士　外川　英明

最終頁に続く

(54)【発明の名称】　通信装置、通信システム及び通信方法

(57)【要約】
【課題】通信カードが同一であって、過去に接続したことのある外部機器と接続する場合には、通信カードが装着されるホスト装置が異なったとしても無線通信リンク確立作業を簡略化することのできる通信装置を提供することにある。
【解決手段】ＳＤカード１３のフラッシュＲＯＭ１１１内にログ情報格納領域１１１ｄを設け、このＳＤカード１３がパソコン１等ホスト装置に装着されて外部機器と無線通信を行った際のログ情報をこのログ情報格納領域１１１ｄに保存する。次にＰＤＡ２１等他のホスト装置から上記同一の外部機器と無線通信する際に上記ログ情報格納領域１１１ｄからログ情報をダウンロードして利用し、無線リンク確立を簡略化する。



1

【特許請求の範囲】

【請求項１】　複数のホスト装置と選択的に通信可能であり、且つホスト装置と外部装置との間のデータ通信を仲介して外部装置との間で無線通信を行う通信手段と、この通信手段が通信した外部機器との通信履歴情報を記憶する記憶手段と、

上記通信手段と外部装置との間で無線通信リンクを確立するものであって、上記記憶手段に通信履歴情報が記憶されていない場合は第１の手順で、上記記憶手段に通信履歴情報が記憶されている場合は上記第１の手順より簡略な第２の手順で、無線通信リンクを確立する確立手段と、を具備することを特徴とする通信装置。

【請求項２】　複数のホスト装置と選択的に通信可能であり、且つホスト装置と外部装置との間のデータ通信を仲介して外部装置との間で無線通信を行う通信手段と、この通信手段が通信した外部機器との通信履歴情報を記憶する記憶手段と、

この記憶手段に記憶された上記通信履歴情報へのアクセスを制限する制限手段と、

この制限手段のアクセス制限を解除する解除手段と、

上記通信手段と外部装置との間の無線リンクを確立するものであって、上記記憶手段に通信履歴情報が記憶されていない場合は第１の手順で、上記記憶手段に通信履歴情報が記憶されて且つ上記解除手段でアクセス制限が解除された場合は上記第１の手順より簡略な第２の手順で、無線通信リンクを確立する確立手段と、を具備することを特徴とする通信装置。

【請求項３】　複数のホスト装置と選択的に通信可能であり、且つホスト装置と外部装置との間のデータ通信を仲介して外部装置との間で無線通信を行う通信手段と、この通信手段が通信した外部機器との通信履歴情報を記憶する記憶手段と、

上記通信手段と外部装置との間で無線通信リンクを確立するものであって、上記記憶手段に通信履歴情報が記憶されていない場合は第１の手順で、上記記憶手段に通信履歴情報が記憶されている場合は上記第１の手順より簡略な第２の手順で、無線通信リンクを確立する確立手段と、

この確立手段による無線通信リンク確立に先立ち、周囲に存在する無線通信可能な機器を探索し、この探索結果情報と上記通信履歴情報とをホスト装置に出力する出力手段と、を具備することを特徴とする通信装置。

【請求項４】　複数のホスト装置と選択的に通信可能であり、且つホスト装置と外部装置との間のデータ通信を仲介し、外部装置との間で無線通信を行う通信手段と、この通信手段と外部装置との間で鍵情報がない場合の第１の手順、及上記鍵情報がある場合の上記第１の手順より簡易な第２の手順のいずれかで無線リンクを確立する確立手段と、

この確立手段が上記第１の手順で無線リンクを確立することに伴い上記鍵情報を生成する生成手段と、

2

この生成手段にて生成された上記鍵情報を記憶する記憶手段と、

上記確立手段が無線リンクを確立する際、外部装置が共通であれば、ホスト装置が変更されることに関わらず、上記記憶手段に記憶された鍵情報を用いて上記第２の手順で行うよう確立手段を制御する制御手段と、

を具備することを特徴とする通信装置。

【請求項５】　複数のホスト装置と選択的に通信可能であり、且つホスト装置と外部装置との間のデータ通信を仲介し、外部装置との間で無線通信を行う通信手段と、この通信手段と外部装置との間で鍵情報がない場合の第１の手順、及上記鍵情報がある場合の上記第１の手順より簡易な第２の手順のいずれかで無線リンクを確立する確立手段と、

この確立手段が上記第１の手順で無線リンクを確立することに伴い上記鍵情報を生成する生成手段と、

この生成手段にて生成された上記鍵情報を記憶する記憶手段と、

この記憶手段に記憶された上記鍵情報へのアクセスを制限する制限手段と、

この制限手段のアクセス制限を解除する解除手段と、

この解除手段でアクセス制限が解除された場合に限り、上記確立手段が無線リンクを確立する際、外部装置が共通であれば、ホスト装置が変更されることに関わらず上記記憶手段に記憶された上記鍵情報を用いて上記第２の手順で行うよう確立手段を制御する制御手段と、

を具備することを特徴とする通信装置。

【請求項６】　複数のホスト装置に対し着脱可能であり、装着されたホスト装置と通信する第１の通信手段と、

ホスト装置に装着された状態で、上記第１の通信手段を介して受領したデータを外部装置との間で無線により通信する第２の通信手段と、

この第２の通信手段が通信した外部機器との通信履歴情報を記憶する記憶手段と、

上記第２の通信手段と外部装置との間で無線通信リンクを確立するものであって、上記記憶手段に通信履歴情報が記憶されていない場合は第１の手順で、上記記憶手段に通信履歴情報が記憶されている場合は上記第１の手順より簡略な第２の手順で、無線通信リンクを確立する確立手段と、を具備し、外部機器が共通であれば、ホスト装置が替わっても上記第２の手順による無線通信リンク確立を実行することを特徴とする通信装置。

【請求項７】　ホスト装置が使用する無線通信用のドライバソフトウェアを記憶する第２の記憶手段を有し、ホスト装置に装着された状態で上記ドライバソフトウェアをホスト装置に出力することを特徴とする請求項６記載の通信装置。

【請求項８】　上記記憶手段に通信履歴情報を記憶する

際、同一の外部機器に対する通信履歴情報が記憶されている場合は、この既に記憶されている通信履歴情報を新たな通信履歴情報に置き替えることを特徴とする請求項６記載の通信装置。

【請求項９】　上記記憶手段に通信履歴情報を記憶する際、記憶容量が不足している場合には、接続日時の最も古い通信履歴情報を新たな通信履歴情報に置き替えることを特徴とする請求項６記載の通信装置。

【請求項１０】　複数のホスト装置に対し着脱可能であり、装着されたホスト装置と通信する第１の通信手段と、

ホスト装置に装着された状態で、上記第１の通信手段を介して受領したデータを外部装置との間で無線により通信する第２の通信手段と、

この第２の通信手段が通信した外部機器との通信履歴情報を記憶する記憶手段と、

この記憶手段に記憶された上記通信履歴情報へのアクセスを制限する制限手段と、

この制限手段のアクセス制限を解除する解除手段と、

上記第２の通信手段と外部装置との間の無線リンクを確立するものであって、上記記憶手段に通信履歴情報が記憶されていない場合は第１の手順で、上記記憶手段に通信履歴情報が記憶されて且つ上記解除手段でアクセス制限が解除された場合は上記第１の手順より簡略な第２の手順で、無線通信リンクを確立する確立手段と、を具備し、外部機器が共通であれば、ホスト装置が替わっても上記第２の手順による無線通信リンク確立を実行することを特徴とする通信装置。

【請求項１１】　上記制限手段は、上記通信履歴情報に対しセキュリティＩＤを設定する設定手段を有し、

上記解除手段は、セキュリティＩＤを入力する入力手段と、この入力手段で入力されたセキュリティＩＤが上記設定手段にて設定されたセキュリティＩＤと一致することを比較する比較手段と、を有することを特徴とする請求項１０記載の通信装置。

【請求項１２】　上記設定手段は複数のセキュリティＩＤを設定し、上記解除手段はこれらのセキュリティＩＤ毎に解除することを特徴とする請求項１１記載の通信装置。

【請求項１３】　複数のホスト装置に対し着脱可能であり、装着されたホスト装置と通信する第１の通信手段と、

ホスト装置に装着された状態で、上記第１の通信手段を介して受領したデータを外部装置との間で無線により通信する第２の通信手段と、

この第２の通信手段が通信した外部機器との通信履歴情報を記憶する記憶手段と、

この記憶手段に記憶された上記通信履歴情報へのアクセスを制限する制限手段と、

この制限手段のアクセス制限を解除する解除手段と、

上記第２の通信手段と外部装置との間の無線リンクを確立するものであって、上記記憶手段に通信履歴情報が記憶されていない場合は第１の手順で、上記記憶手段に通信履歴情報が記憶されて且つ上記解除手段でアクセス制限が解除された場合は上記第１の手順より簡略な第２の手順で、無線通信リンクを確立する確立手段と、

この確立手段による無線通信リンク確立に先立ち、周囲に存在する無線通信可能な機器を探索し、この探索結果情報と上記通信履歴情報とをホスト装置に出力する出力手段と、を具備することを特徴とする通信装置。

【請求項１４】　通信装置とこの通信装置を介して外部機器とデータ通信を行うホスト装置とからなる通信システムにおいて、

上記通信装置は、

上記ホスト装置との間でデータ通信を行う第１の通信手段と、

この第１の通信手段を介して送受されるデータを外部装置との間で無線通信する第２の通信手段と、

この第２の通信手段が通信した外部機器との通信履歴情報を記憶する記憶手段と、

上記第２の通信手段と外部装置との間で無線通信リンクを確立するものであって、上記記憶手段に通信履歴情報が記憶されていない場合は第１の手順で、上記記憶手段に通信履歴情報が記憶されている場合は上記第１の手順より簡略な第２の手順で、無線通信リンクを確立する確立手段と、を有し、

上記ホスト装置は、上記第１の通信手段とデータ通信する通信手段を有することを特徴とする通信システム。

【請求項１５】　通信装置とこの通信装置を介して外部機器とデータ通信を行うホスト装置とからなる通信システムにおいて、

上記通信装置は、

上記ホスト装置との間でデータ通信を行う第１の通信手段と、

この第１の通信手段を介して送受されるデータを外部装置との間で無線通信する第２の通信手段と、

この第２の通信手段が通信した外部機器との通信履歴情報を記憶する記憶手段と、

この記憶手段に記憶された上記通信履歴情報へのアクセスを制限する制限手段と、

この制限手段のアクセス制限を解除する解除手段と、

上記第２の通信手段と外部装置との間で無線通信リンクを確立するものであって、上記記憶手段に通信履歴情報が記憶されていない場合は第１の手順で、上記記憶手段に通信履歴情報が記憶されていて且つ上記解除手段でアクセス制限が解除されている場合は上記第１の手順より簡略な第２の手順で、無線通信リンクを確立する確立手段と、を有し、

上記ホスト装置は、

上記第１の通信手段とデータ通信する通信手段と、

5

上記制限手段がアクセス制限に使用する情報、及び上記解除手段がアクセス制限の解除に使用する情報を入力する入力手段と、を有することを特徴とする通信システム。

【請求項１６】　通信装置とこの通信装置を介して外部機器とデータ通信を行うホスト装置とからなる通信システムにおいて、

上記通信装置は、

上記ホスト装置との間でデータ通信を行う第１の通信手段と、

この第１の通信手段を介して送受されるデータを外部装置との間で無線通信する第２の通信手段と、

この第２の通信手段が通信した外部機器との通信履歴情報を記憶する記憶手段と、

上記第２の通信手段と外部装置との間で無線通信リンクを確立するものであって、上記記憶手段に通信履歴情報が記憶されていない場合は第１の手順で、上記記憶手段に通信履歴情報が記憶されている場合は上記第１の手順より簡略な第２の手順で、無線通信リンクを確立する確立手段と、

この確立手段による無線通信リンク確立に先立ち、周囲に存在する無線通信可能な機器を探索し、この探索結果情報と上記通信履歴情報とを上記第１の通信手段を介して上記ホスト装置へ出力する出力手段と、を有し、

上記ホスト装置は、

上記第１の通信手段とデータ通信する通信手段と、

上記出力手段により出力された上記探索結果情報と上記通信履歴情報とを表示する表示手段と、を有することを特徴とする通信システム。

【請求項１７】　複数のホスト装置と選択的に通信し、且つホスト装置と外部装置との間のデータ通信を仲介して外部装置との間で無線通信を行う通信方法において、

無線通信を行った外部機器との通信履歴情報を記憶し、

外部機器と無線通信リンクを確立する際、当該外部機器に対する上記通信履歴情報が記憶されているかを判断し、

上記通信履歴情報が記憶されていない場合は第１の手順で、上記通信履歴情報が記憶されている場合は上記第１の手順より簡略な第２の手順で無線通信リンクを確立することを特徴とする通信方法。

【請求項１８】　複数のホスト装置と選択的に通信し、且つホスト装置と外部装置との間のデータ通信を仲介して外部装置との間で無線通信を行う通信方法において、

無線通信を行った外部機器との通信履歴情報を記憶し、

記憶した上記通信履歴情報へのアクセスを特定の解除情報がない限り禁止し、

外部機器と無線通信リンクを確立する際、アクセス可能で且つ当該外部機器に対する上記通信履歴情報が記憶されているかを判断し、

上記通信履歴情報が記憶されていない場合は第１の手順で、上記通信履歴情報が記憶されている場合は上記第１の手順より簡略な第２の手順で無線通信リンクを確立することを特徴とする通信方法。

【請求項１９】　複数のホスト装置と選択的に通信し、且つホスト装置と外部装置との間のデータ通信を仲介して外部装置との間で無線通信を行う通信方法において、

無線通信を行った外部機器との通信履歴情報を記憶し、

外部機器と無線通信リンクを確立する際、周囲に存在する無線通信可能な機器を探索し、

探索した結果情報と上記記憶した通信履歴情報とをホスト装置に出力し、

ホスト装置からの外部機器を特定する情報を受け、

上記通信履歴情報が記憶されていない外部機器の場合は第１の手順で、上記通信履歴情報が記憶されている外部機器の場合は上記第１の手順より簡略な第２の手順で無線通信リンクを確立することを特徴とする通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、Ｂｌｕｅｔｏｏｔｈ方式等の通信機能を有し、ホスト装置としての各種電子機器に着脱可能に構成された通信装置、この通信装置とホスト装置とからなる通信システム、及び通信方法に関する。

【０００２】

【従来の技術】近年、パーソナルコンピュータ（以下、パソコンと称する）、携帯型個人情報端末（以下、ＰＤＡと称する）、及び携帯電話等の様々な電子機器が普及している。そして、これら電子機器間のデータ授受をサポートすることを目的として、Ｂｌｕｅｔｏｏｔｈ方式の無線通信機能を持つＰＣＭＣＩＡ規格に準拠したカード（以下、ＰＣカードと称する）やＳＤＭＩセキュリティ準拠のＳＤカードも市場に出はじめている。これらＰＣカードやＳＤカードにとって上記電子機器はホスト装置であり、ホスト装置に装着された状態でホスト装置と外部機器間でデータを仲介するよう無線通信する。Ｂｌｕｅｔｏｏｔｈ方式の場合、通信データに対するセキュリティ向上を目的として、機器間で無線通信リンクを確立する際には相互認証を行うことにより、不特定の者がデータ取得することを防止している。但し、両機器間で１度の無線通信リンクを確立すると、２度目以降無線通信リンク確立作業を簡略化できるため、最初の無線通信時のログ情報をホスト装置の電子機器に記憶し、活用している。

【０００３】しかしながら最近の電子機器の普及率はめざましく、１人の使用者が複数の機器を所有することが珍しくなくなっている。例えば使用者がパソコン、ＰＤＡ、及びＳＤカードを所有している場合、パソコンのデータを外部機器に送信する場合にはＳＤカードをパソコンに装着し、ＰＤＡのデータを外部機器に送信する場合にはＳＤカードをこのＰＤＡに差換えて使用することに

なる。しかしながら、無線通信リンク確立に必要となるログ情報がホスト装置であるパソコン及びＰＤＡのそれぞれに記憶されてしまうため、外部機器が同一のものであってもホスト装置がパソコンからＰＤＡに替わった場合、２度目の無線通信リンク設定であるにも拘わらず、無線通信リンク確立作業を簡略化できない。

【０００４】従来より、無線通信機能を有する着脱可能なカードの側に、送受信履歴を記憶する技術は特開２００１－７７８７８で知られている。しかしながら、この送受信履歴は認証が伴う無線通信リンクの確立手順を簡略化するものではなく、例えこのようなカードを用いたとしても、同じ認証作業を繰り返すことになることになる。

【０００５】

【発明が解決しようとする課題】従来、通信カードは無線接続時の認証に必要なログ情報を記憶せず、パソコン及びＰＤＡ等の電子機器側、つまりホスト装置側が記憶する構成となっていた。このため、使用者が、特定の通信カードを用いて、異なるホスト装置と同一の外部機器とを無線接続する場合、その都度認証を含む無線通信リンク確立作業を行わなければならないという問題があった。

【０００６】そこで本発明は、通信カードが同一であって、過去に接続したことのある外部機器と接続する場合には、通信カードが装着されるホスト装置が異なったとしても無線通信リンク確立作業を簡略化することのできる通信装置、通信システム、及び通信方法を提供することを目的とする。

【０００７】

【課題を解決するための手段】上記目的を達成するため、この発明に係る通信装置は、複数のホスト装置と選択的に通信可能であり、且つホスト装置と外部装置との間のデータ通信を仲介して外部装置との間で無線通信を行う通信手段と、この通信手段が通信した外部機器との通信履歴情報を記憶する記憶手段と、上記通信手段と外部装置との間で無線通信リンクを確立するものであって、上記記憶手段に通信履歴情報が記憶されていない場合は第１の手順で、上記記憶手段に通信履歴情報が記憶されている場合は上記第１の手順より簡略な第２の手順で、無線通信リンクを確立する確立手段と、を具備することを特徴とする。

【０００８】さらにこの発明に係わる通信装置は、複数のホスト装置と選択的に通信可能であり、且つホスト装置と外部装置との間のデータ通信を仲介して外部装置との間で無線通信を行う通信手段と、この通信手段が通信した外部機器との通信履歴情報を記憶する記憶手段と、この記憶手段に記憶された上記通信履歴情報へのアクセスを制限する制限手段と、この制限手段のアクセス制限を解除する解除手段と、上記通信手段と外部装置との間の無線リンクを確立するものであって、上記記憶手段に通信履歴情報が記憶されていない場合は第１の手順で、上記記憶手段に通信履歴情報が記憶されて且つ上記解除手段でアクセス制限が解除された場合は上記第１の手順より簡略な第２の手順で、無線通信リンクを確立する確立手段と、を具備することを特徴とする。

【０００９】上記のように構成された通信装置によれば、過去に接続したことのある外部機器と接続する場合には、通信装置が装着されるホスト装置が異なったとしても無線通信リンク確立作業を簡略化することができる。

【００１０】さらに、通信履歴情報に対するアクセスに制限を加えることができるので、通信装置の紛失や盗難により第三者に渡ってしまったとしても、通信履歴情報を不正にダウンロードされることを防止できる。

【００１１】

【発明の実施の形態】以下図面を参照して本発明の実施の形態について説明する。図１は本実施形態に係わる通信装置、及び外部機器からなる無線通信ネットワークの概略を示す図である。

【００１２】パソコン１は、上面部にキーボード３を備えた本体５と、前面部に表示用のＬＣＤ７を備えた蓋部９とが、ヒンジ部１１を介して開閉可能なノートタイプである。本体５の側面には、ＳＤカード１３を装着するための、ＳＤカードインターフェース仕様に準拠したＳＤカードスロット１５が形成されている。ＳＤカード１３はＢｌｕｅｔｏｏｔｈ方式の無線通信機能を有している。

【００１３】上記パソコン１とは独立した機器であるＰＤＡ２１は、ＬＣＤと透明なタッチセンサパネルとを重畳したタブレット２３を有しており、使用者による入力ペン２５の操作に応じてモード設定やデータ入力等が行われる。ＰＤＡ２１の側面にも、ＳＤカード１３を装着するための、ＳＤカードスロット２７が形成されている。

【００１４】これらパソコン１とＰＤＡ２１は、特定の使用者が所有する機器であり、これに対してパソコン３１、ＦＡＸ３３、プリンタ３５、ＰＤＡ３７、及びパソコン３９は外部機器となる。各外部機器には、ＳＤカード１３が装着時されたパソコン１及びＰＤＡ２１とＢｌｕｅｔｏｏｔｈ方式の無線通信を行うため、それぞれ無線通信部３１ａ、３３ａ、３５ａ、３７ａ、及び３９ａを備えている。

【００１５】例えば、パソコン１で作成したデータをＦＡＸ送信したい場合、ＳＤカード１３と無線通信部３３ａとの間でデータの無線送受信を行い、ＦＡＸ３３は受信したデータを公衆回線を介して所定の相手へＦＡＸ送信する。またパソコン１のデータを印刷したい場合、ＳＤカード１３と無線通信部３５ａとの間でデータの無線送受信を行い、プリンタ３５は受信したデータを紙に印刷する。もし、その後ＰＤＡ２１のデータを印刷したく

なった場合、ＳＤカード１３をＰＤＡ２１に装着し、ＳＤカード１３と無線通信部３５ａとの間でデータの無線送受信を行い、プリンタ３５は受信したデータを紙に印刷する。本実施形態によれば、このプリンタ３５のように外部機器が同一で、且つ同一のＳＤカード１３を使用してパソコン１とＰＤＡ２１のように異なる機器と無線通信する場合、無線リンク確立前の認証作業を簡略化することになる。

【００１６】続いて、本実施形態におけるパソコン１、ＰＤＡ２１、及びＳＤカード１３の具体的な構成を詳細に説明する。

【００１７】パソコン１の本体５は、図２に示すようにパソコン１の動作を制御するＣＰＵ４１を有している。ＣＰＵ４１は、ＣＰＵバス４３及びホスト－ＰＣＩブリッジ４５を介して主メモリ４７、ＶＲＡＭを含むグラフィクスコントローラ４９、及びＰＣＩバス５１に接続している。ＣＰＵ４１は主メモリ４７にロードされるオペレーティングシステム、アプリケーションプログラム、及びＢＩＯＳを実行する。ホスト－ＰＣＩブリッジ４５は、ＣＰＵバス４３とＰＣＩバス５１とを接続するためのバスブリッジであり、さらに主メモリ４７を制御するメモリコントロール機能、及びグラフィクスコントローラ４９との間のデータ転送を行なう機能も備えている。グラフィクスコントローラ４９は、ＬＣＤパネル７に接続している。ＬＣＤパネル７は、グラフィックスコントローラ４９内に設けられた図示しないＶＲＡＭに記憶された情報のパターンデータに基づいて無線通信設定の際のメッセージやアイコン、その他各種情報を表示する。

【００１８】ＰＣＩバス５１には、ＳＤカードコネクタ５２を介してＳＤカード１３とデータ送受信を行なうＳＤホストコントローラ５３、ＰＣカードコネクタ５４を介してＰＣカードとのデータ送受信を行うＰＣホストコントローラ５５、ＰＣＩ－ＩＳＡブリッジ４７、及びＵＳＢ他外部インタフェース５９が接続している。ＳＤカードコネクタ５２は、ＳＤカードスロット１５内に配置され、ＳＤカード１３の装着有無を検出するスイッチ６１を備えている。ＰＣカードコネクタ５４は、本体５に形成されたＰＣカードスロット６３内に設けられている。ＰＣＩ－ＩＳＡブリッジ４７は、ＰＣＩバス５１をＩＳＡバス６５に接続するためのバスブリッジであり、さらに内蔵型のＨＤＤ６７が接続されている。ＨＤＤ６７は、オペレーティングシステム、ＳＤカード１３を使用して無線通信を行うためのドライバソフト等のアプリケーションソフトウェア、及びデータを格納しており、各ソフトウェア及びデータはソフトウェア実行時に主メモリ４７へロードされる。上記ドライバソフトは、ＳＤカード１３が初めて装着された際に自動ダウンロードして保存したものである。またＨＤＤ６７には、ＳＤカード１３を介して外部機器と無線通信した際のログ情報等必要なデータを記憶格納する。

【００１９】ＩＳＡバス６５には、キーボード３、ＢＩＯＳ－ＲＯＭ６９、及びＥｍｂｅｄｄｅｄ　Ｃｏｎｔｒｏｌｌｅｒ（以下、ＥＣと称する）７１が接続されている。キーボード３はアキュポイント等のポインティングデバイスを備えている。さらにＥＣ７１には、電源コントローラ７３、パワースイッチ７５、各種報知用ＬＥＤ７７が接続している。ＢＩＯＳ－ＲＯＭ６９は、パソコン１内の各ハードウェアを制御するためのルーチンを体系化したプログラムであるＢＩＯＳを格納している。ＥＣ７１は、電源コントローラ７３と協動してパソコン１全体及び各デバイスの電源オン／オフを制御する電源シーケンス制御機能を提供する。

【００２０】次にＰＤＡ２１の具体的な構成を図３を用いて説明する。

【００２１】ＰＤＡ２１もパソコン１と同様にＣＰＵ８１を有している。このＣＰＵ８１には内部バス８３を介してフラッシュＲＯＭ８５、ＲＡＭ８７、ＶＲＡＭ８９、ＬＣＤ９１、タッチセンサパネル９３、ＳＤカードコネクタ９４を介してＳＤカード１３とデータ送受信を行うＳＤホストコントローラ９５、及びＥＣ９７が接続している。ＳＤカードコネクタ９４は、ＳＤカードスロット２７内に配置され、ＳＤカード１３の装着有無を検出するスイッチ９９を備えている。ＥＣ９７には、電源コントローラ１０１、パワースイッチ１０３、及び各種報知用のＬＥＤ１０５が接続している。

【００２２】ＣＰＵ８１はＰＤＡ２１全体の制御を司るもので、フラッシュＲＯＭ８５に記憶されたソフトウェアを実行することにより各種機能を実行する。フラッシュＲＯＭ８５は、ＣＰＵ８１を動作させるためのプログラム及び各種初期データを格納するための読込み専用メモリ装置であり、ＳＤカード１３の最初の装着時に自動ダウンロードされる無線通信用のドライバソフトを記憶したり、ＳＤカード１３を介して無線通信した際のログ情報等必要なデータの記憶も行う。ＲＡＭ８７は、ＣＰＵ８１による読み書き可能なメモリ装置であり、各種データを一時的に記憶させる作業領域として使用する。ＬＣＤ９１は、ＶＲＡＭ８９に記憶された情報のパターンデータに基づいて無線通信設定の際のメッセージやアイコン、その他各種情報を表示する。このＬＣＤ９１には、タッチセンサパネル９３が重畳して設けられてタブレット２３を構成し、入力ペン２５の接触によりデータ入力を行なう。ＥＣ９７は、電源コントローラ１０１と協動してＰＤＡ２１全体及び各デバイスの電源オン／オフを制御する電源シーケンス制御機能を提供する。

【００２３】続いてＳＤカード１３の具体的な構成を図４を用いて説明する。

【００２４】ＳＤカード１３には、Ｂｌｕｅｔｏｏｔｈ方式無線通信用の構成としてコントローラ１０１、このコントローラ１０１の動作クロックを生成する水晶発信器１０３、外部機器との間で電波送受信するためのアン

テナ１０５、及び無線通信中であることを報知するＬＥＤ１０７が実装されている。コントローラ１０１はバス１０９を介してフラッシュＲＯＭ１１１及びＳＤ／ＩＯコントローラ１１３に接続している。さらにＳＤ／ＩＯコントローラ１１３は、ＩＯバス１１５を介してＳＤコネクタ１１７に接続し、水晶発信器１１９から供給される動作用クロックにより動作する。ＳＤコネクタ１１７は、ＳＤカード１３表面に設けられた９つの信号ピンを含んでおり、パソコン１のＳＤカードコネクタ５２やＰＤＡ２１のＳＤカードコネクタ９４に物理的に接続し、データ送受信を行う。またホスト装置からこのＳＤカード１３へ、ＳＤコネクタ１１７を介して電力が供給される。

【００２５】コントローラ１０１は、ＩＳＭバンドと称される２．４ＧＨｚ帯の産業用バンドの無線電波によって他の１以上の無線通信装置との間で無線データ通信を行うことが可能な無線通信モジュールであり、周波数ホッピングを用いたスペクトラム拡散方式で近距離無線データ通信を実行する。このコントローラ１０１は、１チップにて実現されており、大きく高周波回路部（以下、ＲＦ部と称する）１２１とベースバンドコントローラ１２３とに分かれる。ＲＦ部１２１は高周波信号の送受信を扱うＲＦトランシーバ回路やＲＦアンプ及びその制御部分を含んでいる。ベースバンドコントローラ１２３は、リンク制御やホッピングパターン制御等を初めとするベースバンド処理を行うための機能モジュールである。そして、ベースバンドコントローラ１２３は、ファームウェアに従ってベースバンド処理を実行するＭＰＵ１２５、作業領域としてのＲＡＭ１２７、無線リンク確立のための制御を行うリンクコントローラ１２９、及びフラッシュＲＯＭ１１１から読み出しＳＤ／ＩＯコントローラ１１３へ送出するデータを一時的に保存するレジスタ１３１を備えている。

【００２６】アンテナ１０５は、セラミック製のチップアンテナにより構成されており、ＲＦ部１２１と電気的に接続し２．４ＧＨｚ帯の無線信号の放射・誘導を行う。

【００２７】フラッシュＲＯＭ１１１は、図５に示すように、カード属性情報領域１１１ａ、ホスト用プログラム領域１１１ｂ、コントローラ用ファームウェア領域１１１ｃ、及びログ情報格納領域１１１ｄの４つの記憶領域を有している。カード属性情報領域１１１ａでは、ＳＤカード１３の属性情報として、例えば無線通信機能を有するＩＯカードであること等の情報を格納している。ホスト用プログラム領域１１１ｂには、ＳＤカード１３を装着した際に、ホスト機器が使用するドライバソフトウェア（以下、ホスト用ドライバと称する）を格納しており、ホスト装置がホスト用ドライバを保持していない場合には、自動的にアップロードされる。この機能はホスト機器が予めホスト用ドライバを持つ必要がなく、ま

たＰＤＡ２１やデジタルカメラのようなソフトウェアのインストールが困難なホスト機器にとっては非常に有用なものとなる。コントローラ用ファームウェア領域１１１ｃには、コントローラ１０１が使用するファームウェアを格納しており、無線通信実行に際してＲＡＭ１２７に読みこまれ、ＭＰＵ１２５によって実行される。

【００２８】ログ情報格納領域１１１ｄは、外部機器との無線通信の履歴及びその無線通信により生じたログ情報を格納する。この領域はさらに、セキュリティＩＤ毎に区切られており、複数の使用者が個別にセキュリティＩＤを設定して、各々個別にログ情報を記憶させ活用できる構成となっている。例えばセキュリティＩＤ（ａ）の領域には、ログ情報Ｌ１、Ｌ２、…が格納されており、セキュリティＩＤ（ｂ）の領域にはログ情報Ｌ３、…が格納されている。各ログ情報は、無線リンク確立した相手機器の機器名称、デバイスアドレス（以下、ＢＤアドレスと称する）、接続時間、接続日時、電話番号、認証に必要なリンクＫｅｙを含んでいる。後述するとおり、次回以降の接続時及びその認証作業の際に特に重要になるのが機器名称とリンクＫｅｙである。

【００２９】ＳＤ／ＩＯコントローラ１１３はパソコン１やＰＤＡ２１といったホスト機器との間のインターフェースを行うためのカードインターフェースであり、１チップＬＳＩにて実現されている。ＳＤ／ＩＯコントローラ１１３は、制御レジスタ１１３ａ、出力データレジスタ１１３ｂ、及び入力データレジスタ１１３ｃを有しており、ホスト機器とコントローラ１０１との通信は、このＳＤ／ＩＯコントローラ１１３を介して行われる。例えば、データをホスト機器に送出する場合には、ＭＰＵ１２５が制御レジスタ１１３ａの特定ビットのデータを変更すると共に、レジスタ１３１のデータを出力データレジスタ１１３ｂに書き込む。ホスト機器側のＣＰＵは、所定の間隔でこの制御レジスタ１１３ａにアクセスし、上記特定ビットの状態から出力データレジスタ１１３ｂにデータがあることを検出すると、出力データレジスタ１１３ｂからデータを取り出すというように動作する。

【００３０】上述した構成のパソコン１とＳＤカード１３とを用いて外部機器であるプリンタ３５と無線通信を行うための一連の動作を説明する。尚、ＰＤＡ２１にＳＤカード１３を装着して外部機器と無線通信する場合も、一連の動作としては基本的に同じである。

【００３１】本実施形態の無線通信動作の全体流れは、図６に示す通りである。

【００３２】パソコン１のＳＤカードスロット１５にＳＤカード１３が装着されると、スイッチ６１がこれを検知し、ホストコントローラ５３からＰＣＩバス５１を経由してＣＰＵ４１へＳＤカード挿入されたことを通知する（ステップＳ１）。ＣＰＵ４１はこの通知を受けると、ＳＤカード１３のフラッシュＲＯＭ１１１のホスト

用プログラム領域１１１ｂに格納されたホスト機器であるパソコン１用のホスト用ドライバがＨＤＤ６７に既にダウンロードされているかを調べる（ステップＳ２）。ホスト用ドライバがダウンロード済であれば、ＣＰＵ４１はキーボード３からホスト用ドライバの起動要求、つまり無線通信実行要求が為されるのを待つ（ステップＳ３）。上記ステップＳ３にてホスト用ドライバのダウンロードが行われていない場合には、ＳＤカード１３からホスト用ドライバをダウンロードして、ＨＤＤ６７に格納し（ステップＳ４）、ステップＳ３へ進む。

【００３３】ステップＳ３で起動要求が為されたと判断すると、ホスト用ドライバを起動する（ステップＳ５）。ホスト用ドライバを起動すると、セキュリティＩＤがＳＤカード１３に設定済であるかを判断する（ステップＳ６）。具体的には、ＣＰＵ４１からＳＤカード１３に対して、フラッシュＲＯＭ１１１のログ情報格納領域１１１ｄにセキュリティＩＤ設定済か否かの問合せを行い、未設定であればＳＤカード１３からＩＤ設定要求が、又設定済であればＩＤ設定済が返送されてくるので、この応答に基づいて判断する。ステップＳ６でセキュリティＩＤ未設定の場合には、セキュリティＩＤ設定フェーズへ進み、セキュリティＩＤを設定する（ステップＳ７）。このセキュリティＩＤを設定することにより、ログ情報に対するアクセスに制限を加えることになり、例えばＳＤカード１３を紛失したり、盗難されたりして第三者の手に渡っても、不正にログ情報がダウンロードされることを防止することになる。

【００３４】一方、ステップＳ６でセキュリティＩＤが設定済であると判断された場合、ホスト用ドライバは、セキュリティＩＤを追加設定するかの問合せ画面をＬＣＤパネル７に表示させ、使用者に追加設定可否入力を促す（ステップＳ８）。ここでセキュリティＩＤ設定要の入力があれば（ステップＳ８）、セキュリティＩＤ設定フェーズへ進み、セキュリティＩＤ設定不要の入力があれば、ログ情報有無確認フェーズへ進んでログ情報の有無を確認する（ステップＳ１０）。このステップＳ１０では、ＳＤカード１３のログ情報格納領域１１１ｄから、セキュリティＩＤに対応したログ情報を取得し、無線通信リンク設定時の認証作業の簡略化を図る。

【００３５】ステップＳ７又はＳ１０の後、ＣＰＵ４１は、接続相手機器を特定した無線通信接続要求が為されたかを判断する（ステップＳ１１）。ステップＳ１１でＣＰＵ４１が接続要求が為されたと判断すると、無線通信リンク設定フェーズへ進み無線通信リンクを設定する（ステップＳ１２）。無線通信リンク設定フェーズでは、ステップＳ７において取得したログ情報、つまり過去に接続した相手機器情報がある場合、これを利用して認証作業を行う。無線通信リンクが設定された上で、対象データを所望の相手機器とＳＤカード１３を介して無線通信する（ステップＳ１３）。無線通信が終了する

と、ＭＰＵ１２５は相手機器との無線通信に関するログ情報を作成し、ログ情報格納領域１１１ｄに格納する（ステップＳ１４）。ログ情報格納時に、既に同一のＢＤアドレスのログ情報があれば、この記憶されたログ情報と新たに作成したログ情報とを置きかえる。また、もし容量的にログ情報格納領域１１１ｄに追加して記憶することが不可能な場合には、接続日時が最も古いものと新たに作成したログ情報とを置きかえるよう動作する。

【００３６】上述したセキュリティＩＤ設定フェーズ、ログ情報有無確認フェーズ、及び無線通信リンク設定フェーズについては、それぞれ図面を参照しつつさらに詳細に説明する。

【００３７】セキュリティＩＤ設定フェーズは、図７乃至図９を用いて説明する。

【００３８】セキュリティＩＤ設定フェーズが開始すると、ＣＰＵ４１はＬＣＤパネル７にセキュリティＩＤ設定画面を表示する（ステップＳ１００）。この設定画面は、例えば図８に示すように、８桁のセキュリティＩＤ入力領域と、「設定実行」「キャンセル」の入力用アイコンを含んでいる。上記セキュリティＩＤは８桁に限るものではなく、その長さは適宜選択、設定できるものである。ステップＳ１００において、所定時間以内、例えば５分以内、にセキュリティＩＤの入力が為されないか又はキャンセルアイコンがクリックされると、ＣＰＵ４１はＳＤホストコントローラ５３に、ＳＤカード１３へ終了コマンドを送出させる（ステップＳ１０１、Ｓ１０２）。終了コマンドの送出とは具体的に述べると、ＳＤ／ＩＯコントローラ１１３の入力データレジスタ１１３Ｃに終了コマンドの情報が書き込むと共に、制御レジスタ１１３ａの中の書込みを示すビットの状態を変化（「０」→「１」）させることである。こうすることによってＭＰＵ１２５が、終了コマンド情報を受け取り、ＳＤカード１３の終了動作を行う（ステップＳ１０３）。以降ＳＤホストコントローラ５３がコマンドや情報をＳＤカード１３に送出すると記載する場合は、上述のようにＳＤ／ＩＯコントローラ１１３の制御レジスタ１１３ａ及び入力データレジスタ１１３ｃにデータを書込むことを意味する。ステップＳ１０２、Ｓ１０３の後パソコン１及びＳＤカード１３はそれぞれ図６の初期状態へ戻る。

【００３９】ステップＳ１０１において、例えば図９に示すようにセキュリティＩＤがキーボード３から入力され、設定実行アイコンがクリックされると、ＣＰＵ４１は書込みコマンドをＳＤホストコントローラ５３からＳＤカード１３へ送出させる（ステップＳ１０４）。書込みコマンドを受領すると、ＳＤカード１３のＭＰＵ１２５は書込み準備を行う（ステップＳ１０５）。ステップＳ１０３に続いてＣＰＵ４１は、キーボード３から入力されたセキュリティＩＤを、ＳＤホストコントローラ５３からＳＤカード１３へ送出させる（ステップＳ１０

６）。ＳＤカード１３のＭＰＵ１２５は、このセキュリティＩＤを受領すると、フラッシュＲＯＭ１１１のログ情報格納領域１１１ｄに格納する（ステップＳ１０７）。セキュリティＩＤの送出後、ＣＰＵ４１は、ＳＤホストコントローラ５３に対し、ＳＤカード１３へ終了コマンドを送出させる（ステップＳ１０８）。ＳＤカード１３のＭＰＵ１２５は、終了コマンドを受領すると終了動作を実行する（ステップＳ１０９）。ステップＳ１０８及びＳ１０９の後、パソコン１及びＳＤカード１３はセキュリティＩＤ設定フェーズを終了する。

【００４０】次に、ログ情報有無確認フェーズについて、図１０乃至図１４を参照して説明する。

【００４１】ログ情報有無確認フェーズが開始すると、ＣＰＵ４１は、ホスト用ドライバに従い、ＬＣＤパネル７にセキュリティＩＤ入力画面表示を行う（ステップＳ２００）。この入力画面は、例えば図１１に示すように、８桁のセキュリティＩＤ入力領域と、「送信」「キャンセル」の入力用アイコンを含んでいる。ステップＳ２００において、所定時間以内、例えば５分以内、にセキュリティＩＤの入力が為されないか又はキャンセルアイコンがクリックされると、ＣＰＵ４１は、ＳＤホストコントローラ５３に、ＳＤカード１３へ終了コマンドを送出させる（ステップＳ２０１、Ｓ２０２）。ＳＤカード１３のＭＰＵ１２５がここで終了コマンドを受領すると、終了動作を行い、ログ情報有無確認フェーズを終了する（ステップＳ２０３）。こうして終了した場合、以降のフローではログ情報が無いものとして処理されることになる。

【００４２】ステップＳ２０１において、例えば図１２に示すようにセキュリティＩＤがキーボード３から入力され、送信アイコンがクリックされると、ＣＰＵ４１は入力されたセキュリティＩＤの情報をＳＤホストコントローラ５３からＳＤカード１３へ送出させる（ステップＳ２０４）。セキュリティＩＤを受信すると、ＳＤカード１３のＭＰＵ１２５は、フラッシュＲＯＭ１１１のログ情報格納領域１１１ｄに格納されたセキュリティＩＤと比較する（ステップＳ２０５）。比較の結果、ログ情報格納領域１１１ｄ内に受信したセキュリティＩＤと一致するものがあるか否かは判断し（ステップＳ２０６）、一致するものがある場合には、アクセス許可情報をＳＤ／ＩＯコントローラ１１３の出力データレジスタ１１３ｂにセットし、出力データレジスタ１１３ｂにデータセットしたことを示す制御レジスタ１１３ａの所定ビットを変更（「０」→「１」）する（ステップＳ２０７）。この状態にすることにより、ＳＤホストコントローラ５３が所定のタイミングで制御レジスタ１１３ａ及び出力データレジスタ１１３ｂにアクセスする際、ＳＤカード１３からデータを取得可能となる。このようにログ情報にアクセスできるようにすることにより、アクセス制限を解除する。ＳＤカード１３側のこのような動作を、以降「情報を提示する」と記載する。

【００４３】ＳＤホストコントローラ５３が、ＳＤ／ＩＯコントローラ１１３にアクセスしてアクセス許可情報を取得すると、ＣＰＵ４１はアクセス許可状態であることをＬＣＤパネル７に、図１３に例示するような形態で表示する（ステップＳ２０８）。そしてＣＰＵ４１は、ＳＤホストコントローラ５３を介して、ＳＤカード１３に対して、ログ情報読込み要求コマンドを送出する（ステップＳ２０９）。読込み要求コマンドを受領するＭＰＵ１２５は、ログ情報格納領域１１１ｄの対応するログ情報をＳＤ／ＩＯコントローラ１１３の出力データレジスタ１１３ｂにセットすることにより提示する（ステップＳ２１０）。ＳＤホストコントローラ５３は出力データレジスタ１１３ｂにアクセスし、ログ情報を読込み主メモリ４７へ転送する（ステップＳ２１１）。このようにしてＳＤカード１３からＳＤホストコントローラ５３へ出力され、主メモリ４７へ転送されるログ情報は、図１４に示す情報から構成されている。

【００４４】一方、ステップＳ２０６でログ情報格納領域１１１ｄに、ＳＤホストコントローラ５３から送出されたセキュリティＩＤと一致するものがないと判断した場合、ＳＤカード１３は不一致情報を提示する（ステップＳ２１２）。ＳＤホストコントローラ５３が、ＳＤ／ＩＯコントローラ１１３にアクセスして不一致情報を取得すると、ＣＰＵ４１はセキュリティＩＤが不一致であり、ログ情報へのアクセスが拒否されたことをＬＣＤパネル７に、図１５に例示するような形態で表示する（ステップＳ２１３）。そしてＣＰＵ４１は、セキュリティＩＤの不一致が３回連続であるかを判断する（ステップＳ２１４）。連続３回に達していない場合は、ステップＳ２００へ戻り、再度セキュリティＩＤの入力を促す。しかし連続３回不一致であると判断された場合には、ステップＳ２０２へ進み、ログ情報無しとしてログ情報有無確認フェーズを終了することになる。

【００４５】上述の通り、ログ情報有無確認フェーズでは、セキュリティＩＤが一致した場合に限りパソコン１側がＳＤカード１３に記憶されたログ情報を取得することができるように動作する。

【００４６】最後に無線通信リンク設定フェーズの詳細について、図１６乃至図１９を参照して説明する。

【００４７】パソコン１のＣＰＵ４１は、まずＳＤホストコントローラ５３に対し、ＳＤカード１３へ問合せ要求送信コマンドを送出する（ステップＳ３００）。問合せ要求送信コマンドを受領すると、コントローラ１０１、つまりＭＰＵ１２５、リンクコントローラ１２９、及びＲＦ部１２１と、アンテナ１０５を介しておよそ半径１０ｍ以内にある周囲の機器へ問合せ要求を送信する（ステップＳ３０１）。これは周囲の無線通信可能な機器を探索することである。Ｂｌｕｅｔｏｏｔｈ方式で通信可能な外部機器がこの問合せ要求を受信すると、問合

せ応答を返信する（ステップＳ３０２、Ｓ３０３）。問合せ応答には、外部機器のデバイスアドレス（以下、ＢＤアドレスと称する）、端末種類、及び無線通信の同期をとるために必要な通信クロック情報が含まれている。ＳＤカード１３が、アンテナ１０５を介して問合せ応答を受信すると、ＭＰＵ１２５は、受信情報つまり周囲の機器の探索結果を提示する（ステップＳ３０４）。このようにしてＳＤカード１３から出力される周囲の機器の探索結果をＳＤホストコントローラ５３が取得すると、主メモリ４７にログ情報が有るか否か判断する（ステップＳ３０５、Ｓ３０６）。ＳＤカード１３から出力されたログ情報が主メモリ４７にある場合には、受信情報のＢＤアドレスと一致する機器、ログ情報にのみ存在する機器、及び受信情報にのみ存在する機器をそれぞれ区別して表示する（ステップＳ３０７）。ＣＰＵ４１はＬＣＤパネル７に、例えば図１７に示すようにログ情報及び受信情報を表示する。受信情報のＢＤアドレスと一致する機器は、プリンタＤ１のようにログ情報と共に通常表示とすることにより受信情報に含まれて現在接続可であることを表示する。このように表示された機器は無線通信リンク設定時の認証作業を短縮できる機器であることを意味する。ログ情報にのみ存在し受信情報にない機器は、ＦＡＸＤ２のように反転表示とした上でログ情報を表示する。このように表示することにより受信情報にはないこと、つまり問合せた時点で周囲に通信可能として存在していないことを示す（圏外を示す）。受信情報にのみ存在する機器は、パソコンＤ３のように通常表示として現在接続可を示すもののログ情報を表示していないため、過去に接続したことのない機器であることを示す。このように、無線通信リンク設定時の認証作業を短縮できる機種とできない機種、さらに短縮可だが接続できない機器とを区別させることができる。

【００４８】ステップＳ３０６において、主メモリ４７にログ情報が無いと判断された場合は、受信情報のみを表示する（ステップＳ３０８）。

【００４９】ステップＳ３０７、又はＳ３０８にてＬＣＤパネル７に表示された機器のいずれかがキーボード３により選択されると（ステップＳ３０９）、ＣＰＵ４１は、その選択入力された機器ＡのＢＤアドレス（例えばプリンタＤ１の「１０－００－２２－３３－４４－５５」）を用いて、ＳＤホストコントローラ５３からＳＤカード１３へ呼出し送信コマンドを送出させる（ステップＳ３１０）。ＳＤカード１３では、コントローラ１０１からアンテナ１０５を介して上記特定のＢＤアドレスを用いて機器Ａへ呼出しを送信する（ステップＳ３１１）。このＢＤアドレスの機器Ａは、呼出しを受信すると、自分のＢＤアドレスを含む呼出し応答を送信する（ステップＳ３１２、Ｓ３１３）。ＳＤカード１３では、この呼出し応答を受信すると、コントローラ１０１は、自機の情報を機器Ａへ無線送信する（ステップＳ３１４、Ｓ３１５）。この自機の情報には、ＳＤカード１３のコントローラ１０１を含む無線通信部にのＢＤアドレス、端末種類、及びクロック情報を含んでいる。機器Ａは、ＳＤカード１３からの情報を受信すると、データを記憶して、受信したことを示す受信通知を無線送信する（ステップＳ３１６、Ｓ３１７）。ＳＤカード１３が受信通知を受信すると、Ｌｉｎｋ　Ｋｅｙの有無、つまりロゴ情報の有無に応じて、異なるステップへ進む（ステップＳ３１８、Ｓ３１９）。Ｌｉｎｋ　Ｋｅｙがある場合には、図１８のＡｕｔｈｅｎｔｉｃａｔｉｏｎステップへ進み、Ｌｉｎｋ　Ｋｅｙが無い場合には、図１９のＰａｉｒｉｎｇステップからＬｉｎｋ　Ｋｅｙ生成ステップへ進む。因みにＬｉｎｋ　Ｋｅｙとは１２８ビットの秘密鍵であり、誤接続防止と盗聴防止の管理のために使用される。このＬｉｎｋ　Ｋｅｙは無線通信リンクを確立に伴い生成される。

【００５０】図１８では、まずＡｕｔｈｅｎｔｉｃａｔｉｏｎステップの中で、ＳＤカード１３内で乱数Ａを発生し、外部の機器Ａに送信する（ステップＳ３２０）。その後ＳＤカード１３と機器Ａとで並行して認証用データの作成を行う（ステップＳ３２１、Ｓ３２２）。認証用データの作成には、ＳＤカード１３と機器Ａとがそれぞれ記憶している同一のＬｉｎｋ　Ｋｅｙ、乱数Ａ、機器ＡのＢＤアドレスとが用いられ、且つ同一の演算により求められる。従って、そこから得られる認証用データは通信異常が無い限り一致するはずである。

【００５１】ステップＳ３２２において認証用データ作成の後、機器Ａは作成した認証用データを無線送信する（ステップＳ３２３）。ＳＤカード１３は認証用データを受信すると、自ら生成した認証用データと比較し、一致しているか否かを判断する（ステップＳ３２４、Ｓ３２５）。比較の結果不一致であれば、機器Ａに対し不一致を通知し、さらにパソコン１に対して認証失敗を提示する（ステップＳ３２６、Ｓ３２７）。ＳＤカード１３はこの状態でステップＳ３１１の呼出し送信の前の状態となる。不一致を受信した機器Ａは、ステップＳ３１２の呼出し受信の前の状態へ戻る（ステップＳ３２８）。ＳＤホストコントローラ５３は、認証失敗の情報を取得すると、ＣＰＵ４１がこれをＬＣＤパネル７に表示し、ステップＳ３１５へ戻る（ステップＳ３２９）。

【００５２】ステップＳ３２５において、認証用データが一致していると判断した場合、ＳＤカード１３は機器Ａに対して認証データの一致を通知する（ステップＳ３３０）。このステップＳ３３０までがＡｕｔｈｅｎｔｉｃａｔｉｏｎステップであり、次にＳＤカード１３と機器Ａとの間で暗号化キー生成すると（ステップＳ３３１）、無線リンクが確立する。ＳＤカード１３のＭＰＵ１２５は、無線リンク確立したことを提示し、ＳＤホストコントローラ５３がこの情報を取得すると、ＣＰＵ４１はＬＣＤパネル７に無線リンク確立したことを表示す

る（ステップＳ３３２、Ｓ３３３）。こうしてログ情報がある場合の無線通信リンク設定フェーズを終了する。

【００５３】これに対しステップＳ３１９において、Ｌｉｎｋ　Ｋｅｙが無い、つまりログ情報が無いと判断された場合の無線リンク設定フェーズの後段部分について図１９を用いて説明する。

【００５４】まずＰａｉｒｉｎｇステップの中で、ＳＤカード１３内で乱数Ｃを発生し、外部の機器Ａに送信する（ステップＳ３５０）。機器Ａは乱数Ｃを受信するとＳＤカード１３へ受信確認を送信し、図示しない表示部にＰＩＮコード入力要求を表示する（ステップＳ３５１、Ｓ３５２）。ＰＩＮコードとは、使用者が任意に設定することのできる８ビットのコードである。Ｌｉｎｋ　Ｋｅｙを持たない機器同士で無線通信リンクを確立する場合、誤接続を防止や盗聴防止のために、それぞれの機器から同一のＰＩＮコード入力を行うようになっている。

【００５５】ステップ３５２の表示の後、特定のＰＩＮコードが入力されると、このＰＩＮコード、乱数Ｃ、及び自機（機器Ａ）のＢＤアドレスから仮のＬｉｎｋ　Ｋｅｙを生成する（ステップＳ３５３、Ｓ３５４）。

【００５６】ステップＳ３５１にて機器Ａが送信した受信確認をＳＤカード１３がアンテナ１０５を介して受信すると、ＭＰＵ１２５はＰＩＮコード入力要求情報を提示する（ステップＳ３５５）。ＳＤホストコントローラ５３がＳＤ／ＩＯコントローラ１１３からＰＩＮコード入力要求情報を取得すると、ＣＰＵ４１は、ＬＣＤパネル７にＰＩＮコード要求画面を表示する（ステップＳ３５６）。キーボード３によりＰＩＮコードが入力されると、ＣＰＵ４１はこのＰＩＮコードをＳＤホストコントローラ５３を介してＳＤカード１３へ送出する（ステップＳ３５７、Ｓ３５８）。ここで入力されるＰＩＮコードは、ステップＳ３５３にて機器Ａ側で入力有を判断したＰＩＮコードと同一でなければ、無線通信リンクは確立できない。

【００５７】ＳＤカード１３のＭＰＵ１２５は、受領したＰＩＮコード、乱数Ｃ、及び相手機器ＡのＢＤアドレスから仮のＬｉｎｋ　Ｋｅｙを生成する（ステップＳ３５９）。続いてＳＤカード１３は、乱数Ｄを生成して機器Ａへ送信し、さらにこの乱数Ｄ、ステップＳ３５９で生成した仮Ｌｉｎｋ　Ｋｅｙ、及び機器ＡのＢＤアドレスから認証用データを生成する（ステップＳ３６０、Ｓ３６１）。

【００５８】ＳＤカード１３から乱数Ｂを受信すると、機器ＡでもＳＤカード１３と並行してステップＳ３６１と同様に認証用データの作成を行う（ステップＳ３６２）。ステップＳ３６１及びＳ３６２での認証用データ作成は、ＳＤカード１３と機器Ａとがそれぞれ記憶している、ＰＩＮコードが同一であれば同一であるはずの仮Ｌｉｎｋ　Ｋｅｙ、乱数Ｂ、及び機器ＡのＢＤアドレス

が用いられ、所定の演算により求められる。つまりここでは同じ変数を用いて同じ演算を行うので、そこから得られる認証用データは一致するはずである。

【００５９】ステップＳ３６２において認証用データ作成の後、機器Ａは作成した認証用データを無線送信する（ステップＳ３６３）。ＳＤカード１３は認証用データを受信すると、自ら生成した認証用データと比較し、一致しているか否かを判断する（ステップＳ３６４、Ｓ３６５）。比較の結果不一致であれば、機器Ａに対し不一致を通知し、さらにパソコン１に対して認証失敗を提示する（ステップＳ３６６、Ｓ３６７）。ＳＤカード１３はこの状態でステップＳ３１１の呼出し送信の前の状態となる。不一致を受信した機器Ａは、ステップＳ３１２の呼出し受信の前の状態へ戻る（ステップＳ３６８）。ＳＤホストコントローラ５３は、認証失敗の情報を取得すると、ＣＰＵ４１がこれをＬＣＤパネル７に表示し、ステップＳ３１５へ戻る（ステップＳ３６９）。

【００６０】ステップＳ３６５で認証用データの一致を判断すると、ＳＤカード１３は、機器Ａへ一致を通知する（ステップＳ３７０）。このＰａｉｒｉｎｇステップは、このステップＳ３７０で終了し、次にＬｉｎｋ　Ｋｅｙ生成ステップへ進む。ステップＳ３７０の後、ＳＤカード１３は乱数Ｅを発生し、この発生した乱数Ｅ、自機のＢＤアドレス、及び仮Ｌｉｎｋ　ＫｅｙからＬｉｎｋ　Ｋｅｙ（Ａ）を生成する（ステップＳ３７１、Ｓ３７２）。

【００６１】一方ＳＤカード１３から認証用データの一致の通知を受けると、機器Ａ側でも独立して乱数Ｆを発生し、この乱数Ｆ、自機のＢＤアドレス、及び仮ＬｉｎｋＫｅｙからＬｉｎｋ　Ｋｅｙ（Ｂ）を生成する（ステップＳ３７３、Ｓ３７４）。Ｌｉｎｋ　Ｋｅｙ（Ａ）及びＬｉｎｋ　Ｋｅｙ（Ｂ）は、それぞれ異なる乱数及びＢＤアドレスにより求められるため、一致することは無い。ＳＤカード１３と機器Ａとは、互いにＬｉｎｋ　Ｋｅｙ（Ａ）及び（Ｂ）を相手に送信して共有した後、予め決められたルールに従いＬｉｎｋ　Ｋｅｙ（Ａ）及び（Ｂ）のいずれをＬｉｎｋ　Ｋｅｙとするかを決める（ステップＳ３７５、Ｓ３７６、Ｓ３７７）。

【００６２】このステップＳ３７７までがＬｉｎｋ　Ｋｅｙ生成ステップであり、次にＳＤカード１３と機器Ａとの間で暗号化キーを生成すると（ステップＳ３７８）、無線リンクが確立する。ＳＤカード１３のＭＰＵ１２５は、無線リンク確立したことを提示し、ＳＤホストコントローラ５３がこの情報を取得すると、ＣＰＵ４１はＬＣＤパネル７に無線リンク確立したことを表示する（ステップＳ３７９、Ｓ３８０）。こうしてログ情報が無い場合の無線通信リンク設定フェーズを終了する。

【００６３】図１８では、図１９における認証作業の中でＰＩＮコード入力に伴う部分がなく、またＬｉｎｋ　Ｋｅｙ生成ステップに相当する箇所も無い。このように

図１８は図１９に比較して明らかに短縮化した流れとなっている。

【００６４】上記パソコン１からＳＤカード１３を取り外し、ＰＤＡ２１に装着して無線通信にしようする場合、ログ情報の活用を含め制御の流れは上記説明と同様である。つまり、パソコン１のキーボード３をＰＤＡ２１の入力ペン２５とタッチセンサパネル９３へ、ＬＣＤパネル7をＬＣＤ９１へ、ＣＰＵ４１をＣＰＵ８１へ、主メモリ４７をＲＡＭ８７へ、ＳＤホストコントローラ５３をＳＤホストコントローラ９５、ＨＤＤ６７をフラッシュＲＯＭ８５へ、ＰＣＩバス８１を内部バス８３へ、それぞれ置き換えると、図６乃至図１９において説明した内容と同じ流れとなる。

【００６５】以上詳述した通り、ＳＤカード１３のフラッシュＲＯＭ１１１内にログ情報格納領域１１１ｄを設け、このＳＤカード１３がパソコン１等ホスト装置に装着されて外部機器と無線通信を行った際のログ情報をこのログ情報格納領域１１１ｄに保存する。次にＰＤＡ２１等他のホスト装置から上記同一の外部機器と無線通信する際に上記ログ情報格納領域１１１ｄからログ情報をダウンロードして利用する。従って、ホスト装置が変わってもＳＤカード１３と接続先の外部機器とが同一であれば、無線リンク確立を簡略化することができる。

【００６６】なお、この発明は上述した実施の形態に限定されることなく、この発明の主旨を逸脱しない範囲で種々変形可能である。例えば、通信装置はＳＤカードでなくＰＣカードであっても構わない。この場合ＰＣカードに不揮発性メモリを設け、その中にログ情報格納領域を設定すれば、上記ＳＤカードの場合と同様にＰＣカードスロットを有するホスト装置間での装着変更に拘わらず、無線リンク確立の簡略化を図ることが出来る。

【００６７】また複数のセキュリティＩＤでなく、単一のセキュリティＩＤのみを設定するようにしてもよい。

【００６８】無線通信方式は、Ｂｌｕｅｔｏｏｔｈ方式に限らず、無線リンク設定時にログ情報、特に鍵情報の有無によって異なる手順で動作するものであれば構わない。

【００６９】

【発明の効果】以上詳述したように、本発明によれば、過去に接続したことのある外部機器と接続する場合には、通信装置が装着されるホスト装置が異なったとしても無線通信リンク確立作業を簡略化することができる。

【００７０】さらに、通信履歴情報に対するアクセスに制限を加えることができるので、通信装置の紛失や盗難により第三者に渡ってしまったとしても、通信履歴情報を不正にダウンロードされることを防止できる。

【図面の簡単な説明】

【図１】この発明の実施の形態に係る無線通信ネットワークを示す図。

【図２】同実施形態におけるパーソナルコンピュータの構成を示すブロック図。

【図３】同実施形態におけるＰＤＡの構成を示すブロック図。

【図４】同実施形態のＳＤカードの流れを示す図。

【図５】本実施形態のフラッシュＲＯＭ内のデータ構造を示す図。

【図６】本実施形態の無線通信動作の全体の流れを示す図。

【図７】無線通信動作のセキュリティＩＤ設定フェーズの流れを示す図。

【図８】セキュリティＩＤ設定フェーズにおけるセキュリティＩＤ設定画面を示す図。

【図９】セキュリティＩＤ設定画面でセキュリティＩＤを入力した状態を示す図。

【図１０】無線通信動作のログ情報確認フェーズの流れを示す図。

【図１１】ログ情報確認フェーズにおけるセキュリティＩＤ入力画面を示す図。

【図１２】セキュリティＩＤ入力画面でセキュリティＩＤを入力した状態を示す図。

【図１３】セキュリティＩＤ入力後のログ情報に対するアクセス許可の表示例を示す図。

【図１４】ログ情報確認フェーズでＳＤカードから出力されるログ情報を示す図。

【図１５】セキュリティＩＤ入力後のログ情報に対するアクセス拒否の表示例を示す図。

【図１６】無線通信動作の無線通信リンク設定フェーズの流れを示す図。

【図１７】無線通信リンク設定フェーズにおけるログ情報と受信情報の表示例を示す図。

【図１８】無線通信動作の無線通信リンク設定フェーズの簡略化した無線リンク確立手順の流れを示す図。

【図１９】無線通信動作の無線通信リンク設定フェーズの簡略化しない無線リンク確立手順の流れを示す図。

【符号の説明】

１…パーソナルコンピュータ
３…キーボード
7…ＬＣＤパネル
１３…ＳＤカード
１５…ＳＤカードスロット
２１…ＰＤＡ
２７…ＳＤカードスロット
４１…ＣＰＵ
４７…主メモリ
５３…ＳＤホストコントローラ
１０５…アンテナ
１１１…フラッシュＲＯＭ
１１１ｄ…ログ情報格納領域
１１３…ＳＤ／ＩＯコントローラ
１２１…ＲＦ部

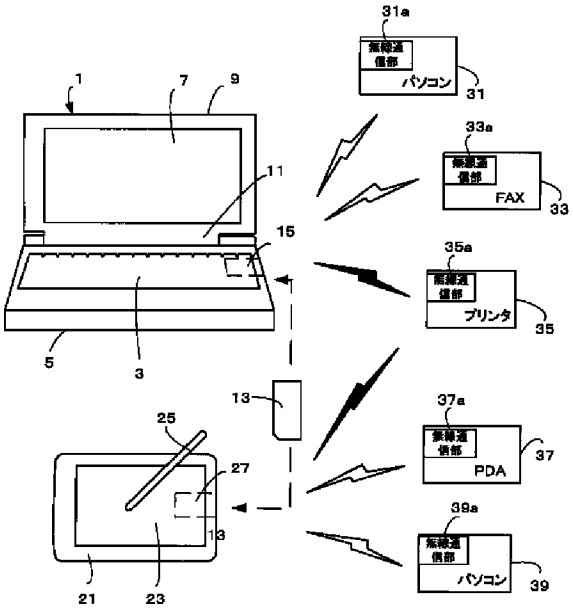
23

１２３…ベースバンドコントローラ

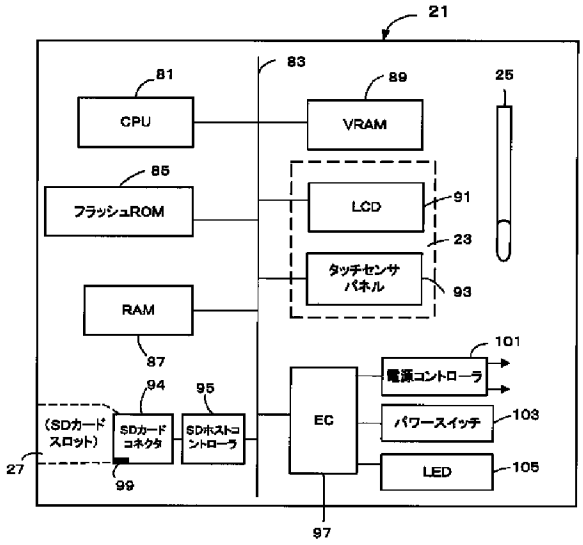
24

＊　＊１２５…ＭＰＵ

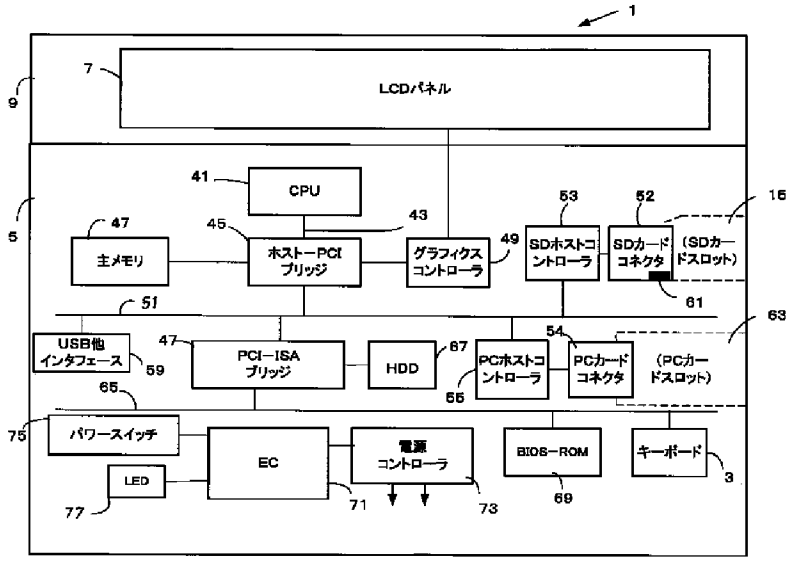
【図１】



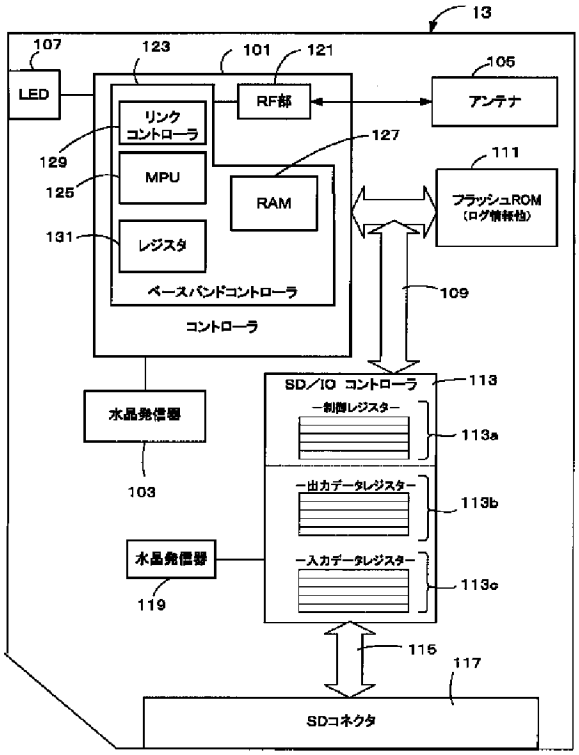
【図３】



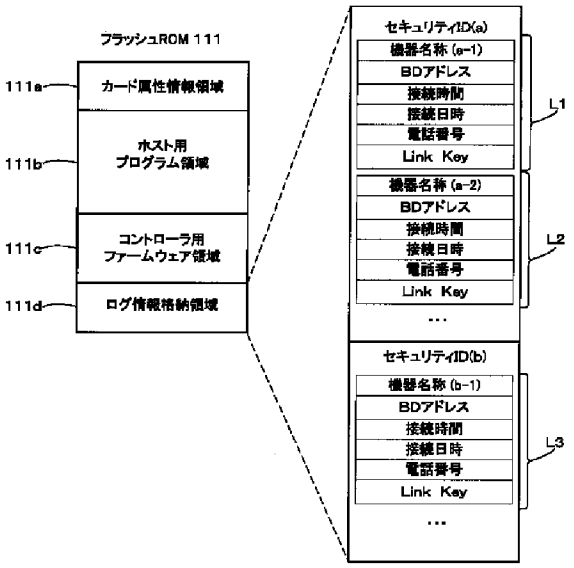
【図２】



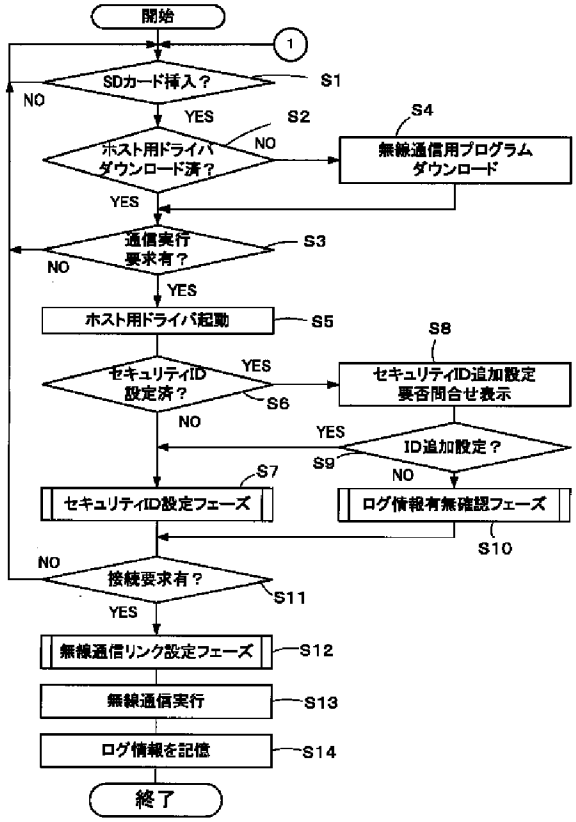
【図４】


13
107
123
101
121
105
LED
リンク
コントローラ
RF部
アンテナ
129
127
111
125
MPU
RAM
フラッシュROM
（ログ情報格納）
131
レジスタ
ベースバンドコントローラ
109
コントローラ
SD／IO コントローラ
113
水晶発信器
制御レジスター
113a
出力データレジスター
113b
103
水晶発信器
入力データレジスター
113c
119
115
117
SDコネクタ

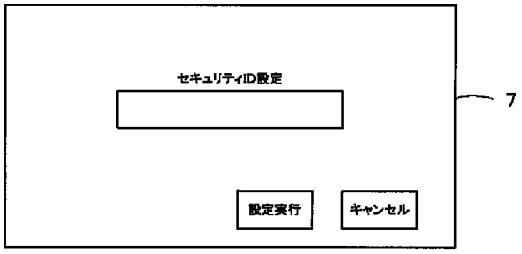
【図５】


フラッシュROM 111
111a
カード属性情報領域
111b
ホスト用
プログラム領域
111c
コントローラ用
ファームウェア領域
111d
ログ情報格納領域
セキュリティID(a)
機器名称 (a-1)
BDアドレス
接続時間
接続日時
電話番号
Link Key
L1
機器名称 (a-2)
BDアドレス
接続時間
接続日時
電話番号
Link Key
L2
セキュリティID(b)
機器名称 (b-1)
BDアドレス
接続時間
接続日時
電話番号
Link Key
L3

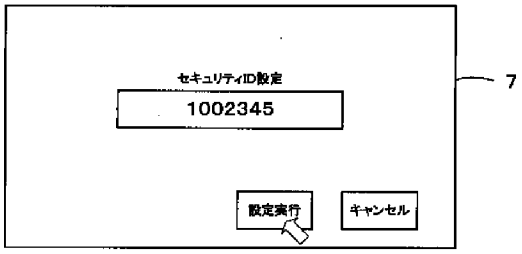
【図６】


開始
1
SDカード挿入？
S1
NO
YES
S2
ホスト用ドライバ
ダウンロード済？
NO
S4
無線通信用プログラム
ダウンロード
YES
通信実行
要求有？
S3
NO
YES
ホスト用ドライバ起動
S5
S8
セキュリティID
設定済？
YES
S6
セキュリティID追加設定
要否問合せ表示
NO
YES
ID追加設定？
S9
NO
S7
セキュリティID設定フェーズ
ログ情報有無確認フェーズ
S10
NO
接続要求有？
S11
YES
無線通信リンク設定フェーズ
S12
無線通信実行
S13
ログ情報を記憶
S14
終了

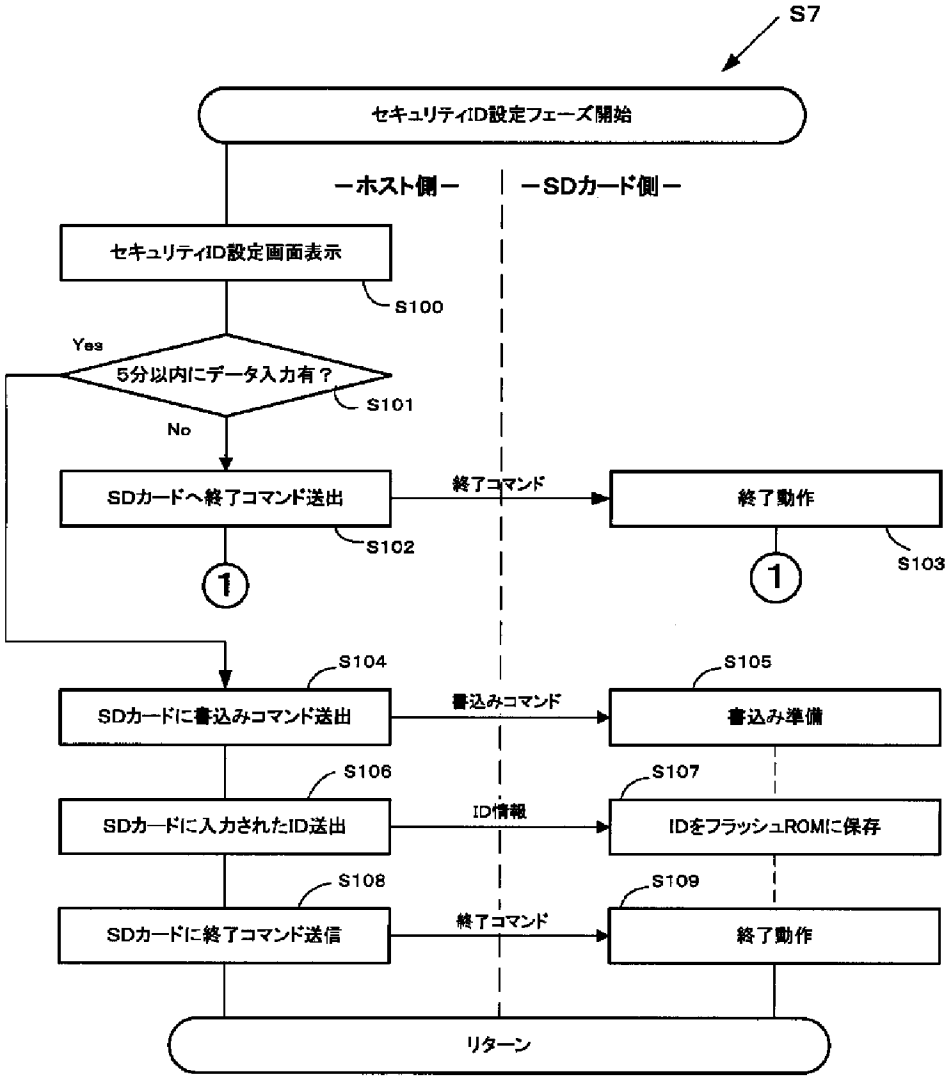
【図８】


セキュリティID設定
7
設定実行
キャンセル

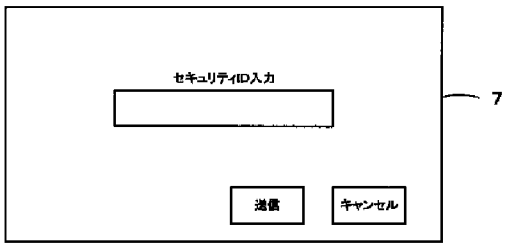
【図９】


セキュリティID設定
1002345
7
設定実行
キャンセル

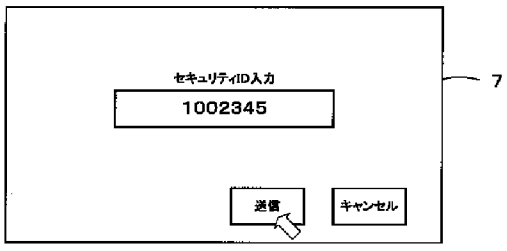
【図７】


S7
セキュリティID設定フェーズ開始
－ホスト側－
－SDカード側－
セキュリティID設定画面表示
S100
Yes
5分以内にデータ入力有？
S101
No
SDカードへ終了コマンド送出
終了コマンド
終了動作
S102
S103
①
①
S104
S105
SDカードに書込みコマンド送出
書込みコマンド
書込み準備
S106
S107
SDカードに入力されたID送出
ID情報
IDをフラッシュROMに保存
S108
S109
SDカードに終了コマンド送信
終了コマンド
終了動作
リターン

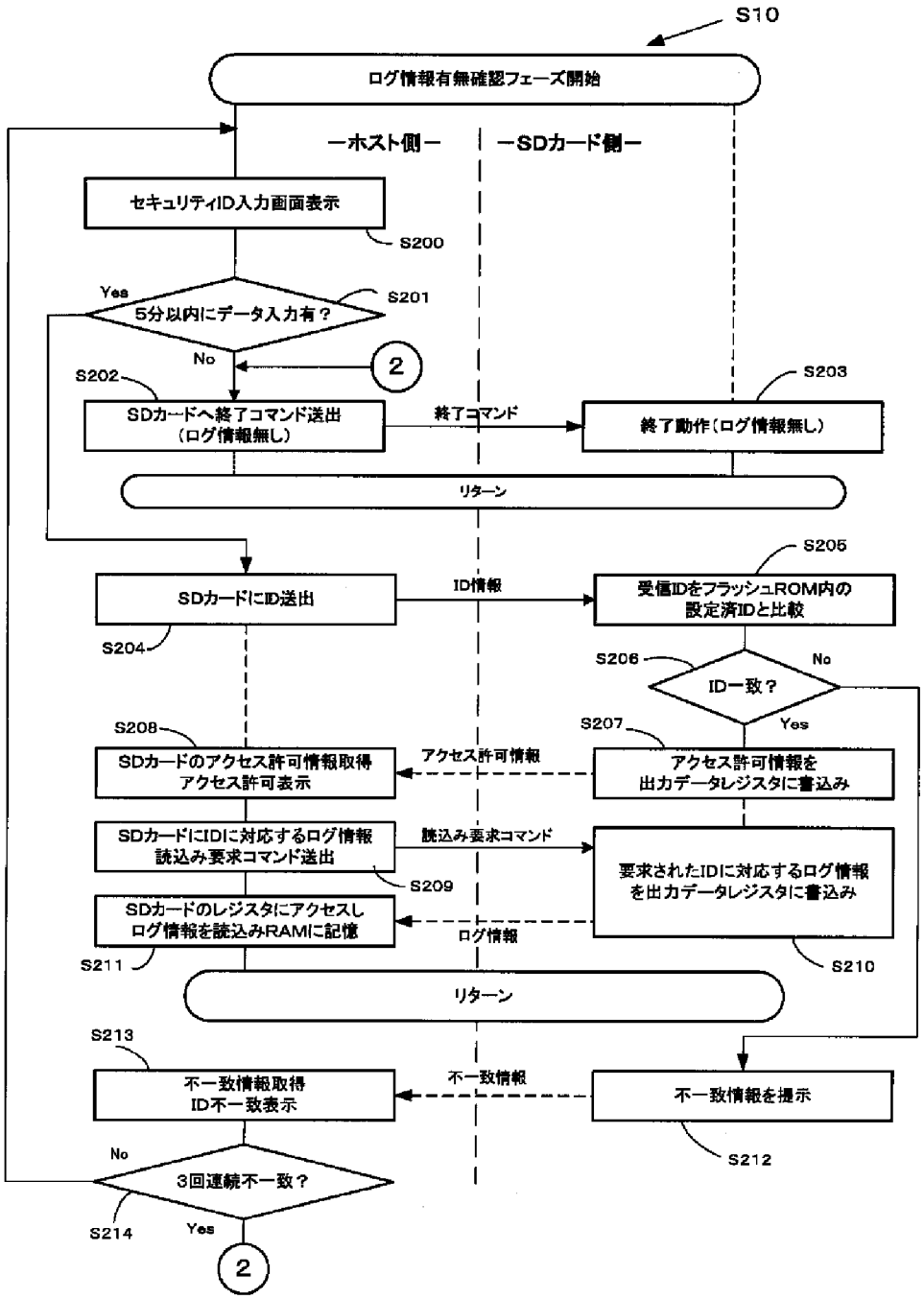
【図１１】


セキュリティID入力
7
送信
キャンセル

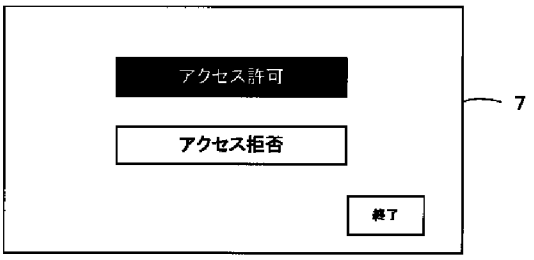
【図１２】


セキュリティID入力
1002345
7
送信
キャンセル

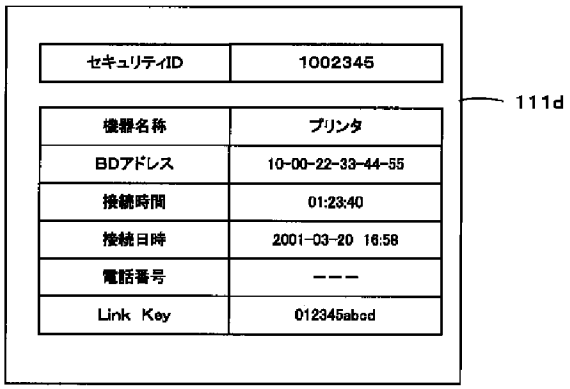
【図１０】


S10
ログ情報有無確認フェーズ開始
－ホスト側－
－SDカード側－
セキュリティID入力画面表示
S200
Yes
5分以内にデータ入力有？
S201
No
2
S202
SDカードへ終了コマンド送出
（ログ情報無し）
終了コマンド
S203
終了動作（ログ情報無し）
リターン
S205
SDカードにID送出
ID情報
受信IDをフラッシュROM内の
設定済IDと比較
S204
S206
No
ID一致？
Yes
S208
S207
SDカードのアクセス許可情報取得
アクセス許可表示
アクセス許可情報
アクセス許可情報を
出力データレジスタに書込み
SDカードにIDに対応するログ情報
読込み要求コマンド送出
読込み要求コマンド
S209
要求されたIDに対応するログ情報
を出力データレジスタに書込み
SDカードのレジスタにアクセスし
ログ情報を読込みRAMに記憶
ログ情報
S211
S210
リターン
S213
不一致情報取得
ID不一致表示
不一致情報
不一致情報を提示
S212
No
3回連続不一致？
S214
Yes
2

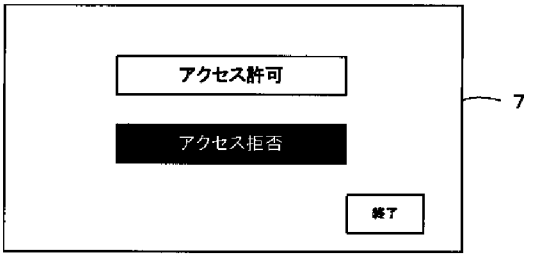
【図１３】



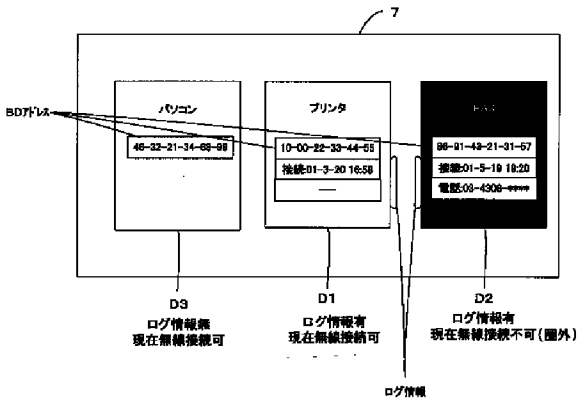
【図１４】



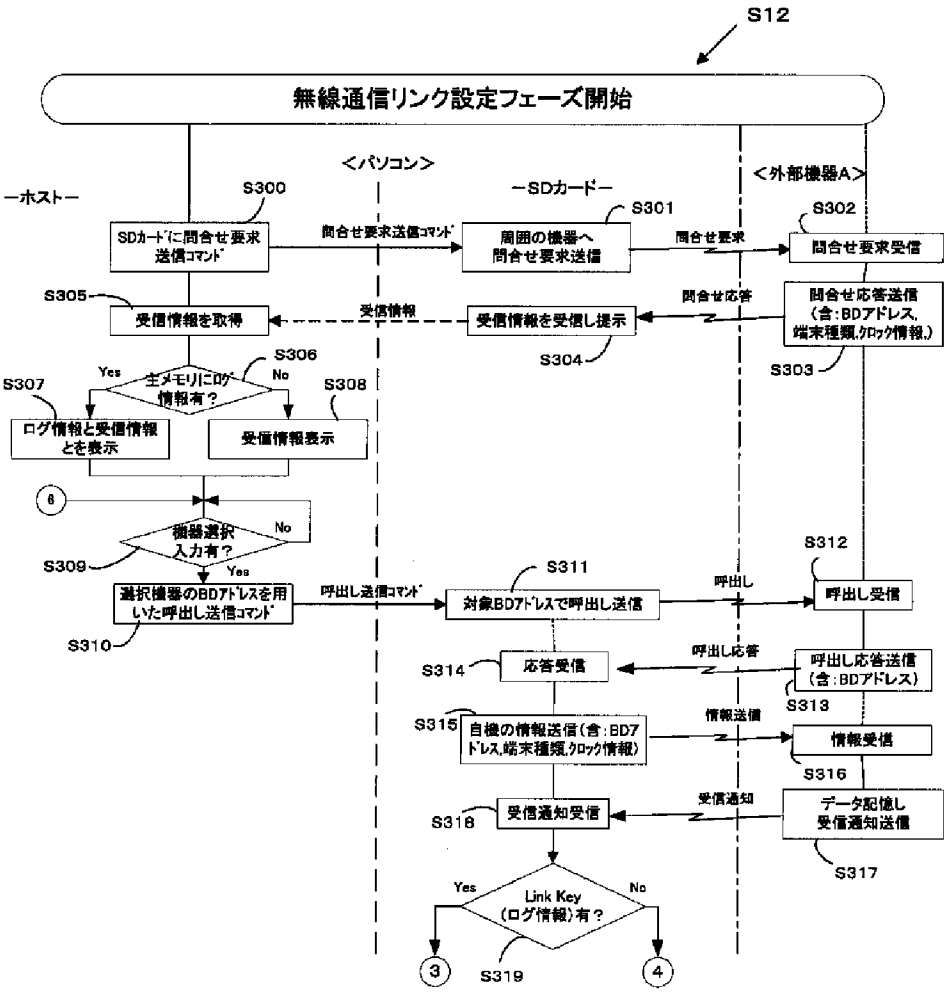
【図１５】



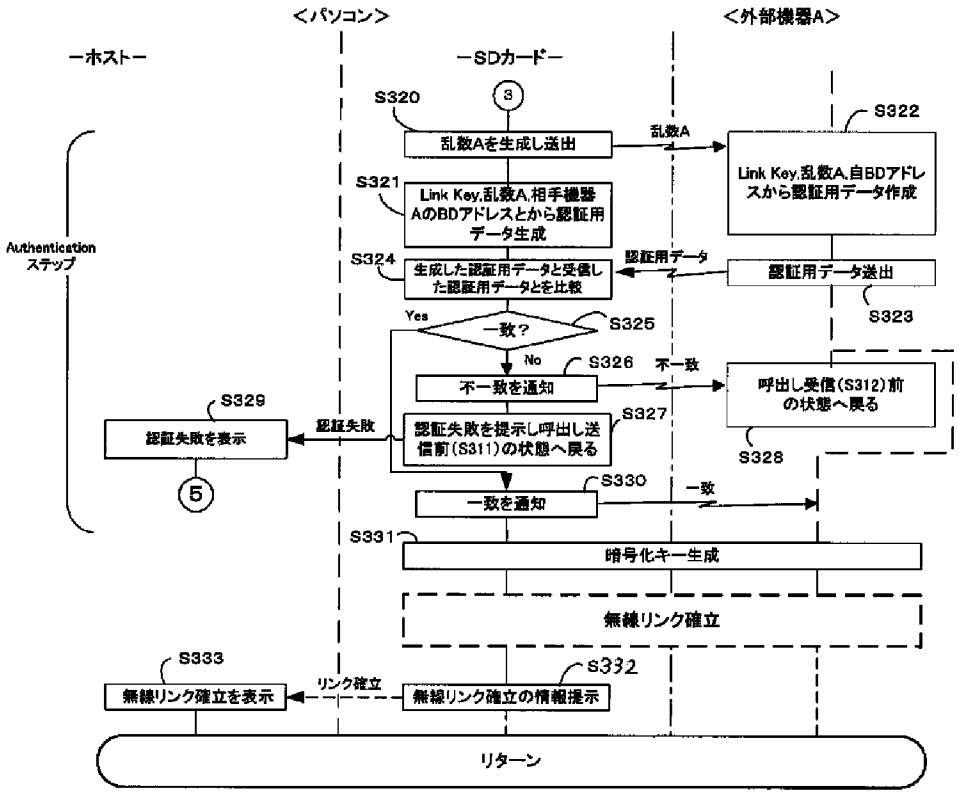
【図１７】



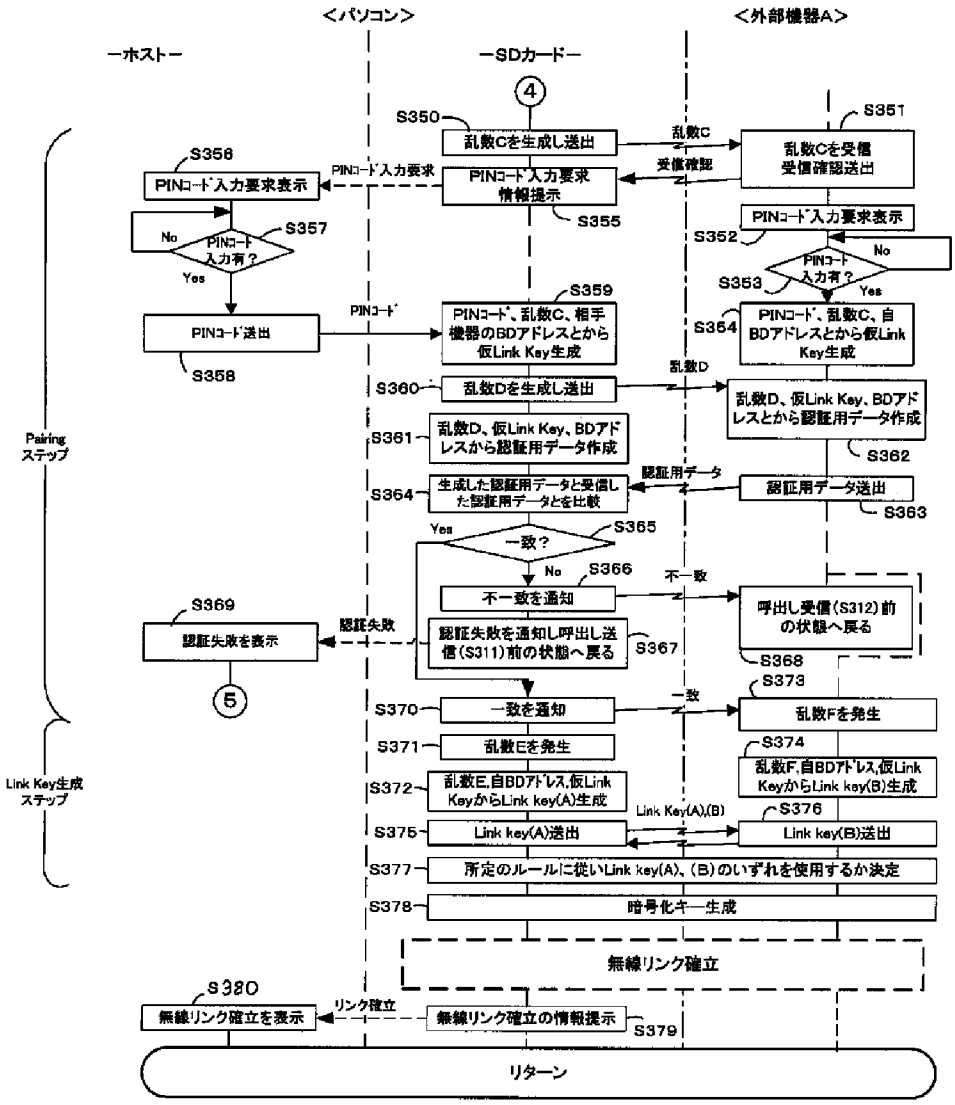
【図１６】


S12
無線通信リンク設定フェーズ開始
<パソコン>
ーホストー
ーSDカードー
<外部機器A>
S300
SDカードに問合せ要求送信コマンド
問合せ要求送信コマンド
S301
周囲の機器へ問合せ要求送信
問合せ要求
S302
問合せ要求受信
S305
受信情報を取得
受信情報
受信情報を受信し提示
問合せ応答
問合せ応答送信（含：BDアドレス，端末種類，クロック情報，）
S304
S303
S306
Yes
主メモリにログ情報有？
No
S307
S308
ログ情報と受信情報とを表示
受信情報表示
6
機器選択入力有？
No
Yes
S309
S312
S311
選択機器のBDアドレスを用いた呼出し送信コマンド
呼出し送信コマンド
対象BDアドレスで呼出し送信
呼出し
呼出し受信
S310
S314
応答受信
呼出し応答
呼出し応答送信（含：BDアドレス）
S313
S315
自機の情報送信（含：BDアドレス，端末種類，クロック情報）
情報送信
情報受信
S316
S318
受信通知受信
受信通知
データ記憶し受信通知送信
S317
Yes
Link Key（ログ情報）有？
No
3
S319
4

【図１８】


<パソコン>
<外部機器A>
ーホストー
ーSDカードー
Authentication ステップ
S320
3
乱数Aを生成し送出
乱数A
S322
Link Key,乱数A,自BDアドレスから認証用データ作成
S321
Link Key,乱数A,相手機器AのBDアドレスとから認証用データ生成
S324
生成した認証用データと受信した認証用データとを比較
認証用データ
認証用データ送出
S323
Yes
一致?
S325
No
S326
不一致を通知
不一致
呼出し受信(S312)前の状態へ戻る
S328
S329
認証失敗を表示
認証失敗
認証失敗を提示し呼出し送信前(S311)の状態へ戻る
S327
5
S330
一致を通知
一致
S331
暗号化キー生成
無線リンク確立
S333
無線リンク確立を表示
リンク確立
S332
無線リンク確立の情報提示
リターン

【図１９】



フロントページの続き

Ｆターム(参考) 5C062 AA02 AA14 AA27 AA37 AB38
AB42 AC22 AC34 AC58 AF00
BD09
5K033 AA08 AA09 DA19 DB12 DB14
5K034 AA19 DD02 EE03 KK21
5K067 AA21 BB02 EE02 EE10 EE16
GG06 HH12 HH22 HH24